Cyber Thursdays

The Federal Cybersecurity Horizon: Zero Trust, FedRAMP, and Supply Chain Risk

August 28 | 11:00 am - Noon

Presented by:

Matt Frost, Wisconsin Procurement Institute

WPI Wisconsin Procurement Institute
An APEX Accelerator

APEX ACCELERATORS

Wisconsin Procurement Institute

An APEX Accelerator

Assisting Wisconsin businesses compete in the government marketplace.

WPI is Wisconsin's APEX ACCELERATOR

The APEX Accelerators program, under management of the Department of Defense (DOD) Office of Small Business Programs (OSBP), plays a critical role in the Department's efforts to identify and engage with a wide range of businesses entering and participating in the defense supply-chain. The program provides the education and training that all businesses need to participate to become capable of participating in DOD and other government contracts.

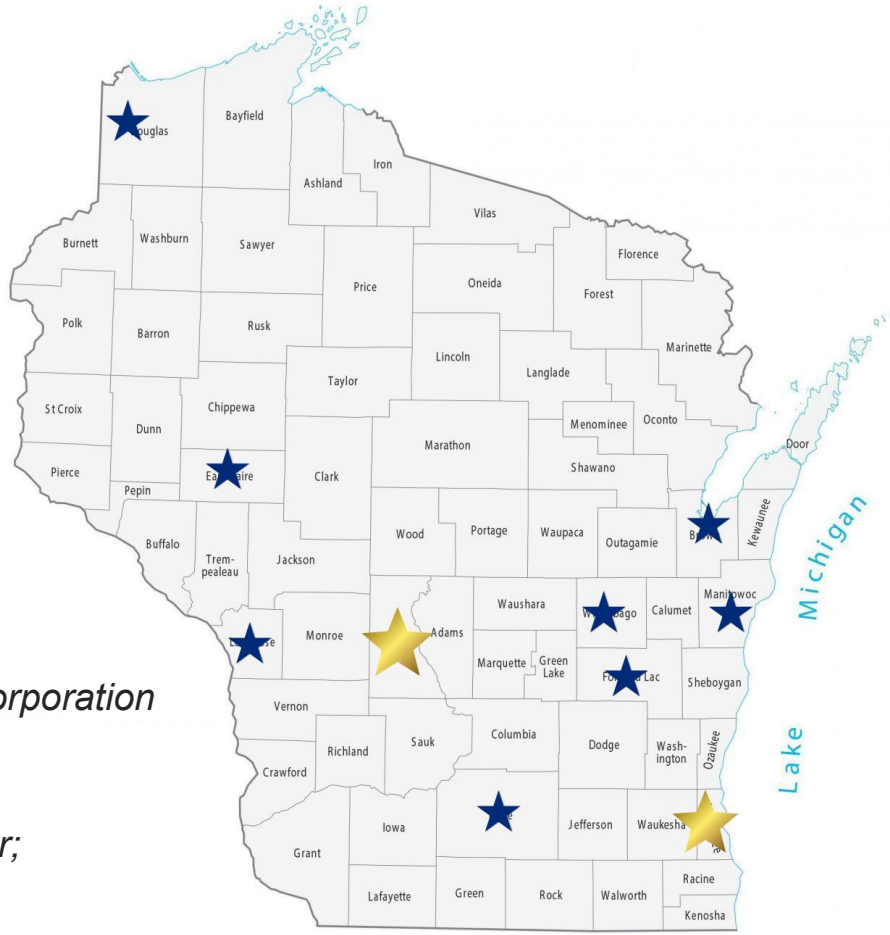
WPI provides services and training to all of Wisconsin's 72 counties

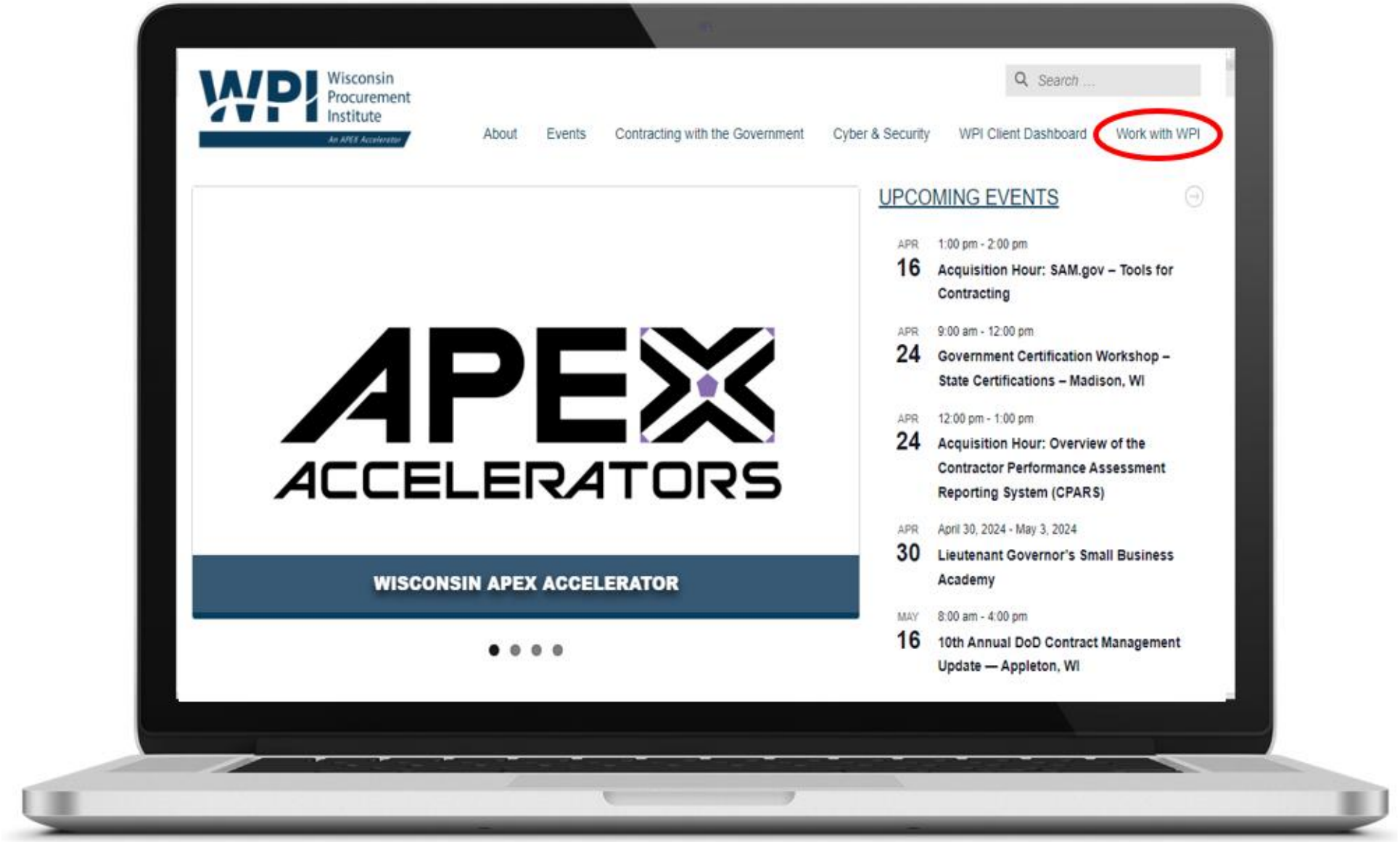
- Individual counseling at our offices, client's facility or virtually
- Small group training – webinars and workshops including Acquisition Hours, Cyber Fridays, Evening FAR sessions, Federal Market Insights and Local Government Sales Opportunities
- Conferences the Governors Marketplace, The Contracting Academy (TCA), WEDCs Small Business Academy, Wisconsin Federal Contractor Forum [DC and in-state], Government Opportunities Business Conference GOBC) with WI military bases, End of Year Federal Contractor Update, Annual DOD Contract Management Update, and more……

www.wispro.org

WPI OFFICE LOCATIONS

- **MILWAUKEE**
  - *Technology Innovation Center*
- **MADISON**
  - *FEED Kitchens*
  - *Dane County Latino Chamber of Commerce*
  - *Wisconsin Manufacturing Extension Partnership (WMEP)*
  - *Madison Area Technical College (MATC)*
- **CAMP DOUGLAS**
  - *Juneau County Economic Development Corporation (JCEDC)*
- **EAU CLAIRE**
  - *Western Dairyland*
- **FOND DU LAC**
  - *Envision Greater Fond du Lac*
- **GREEN BAY**
  - *NWTC Startup Hub*
- **LACROSSE**
  - *Veterans in Professions*
- **MANITOWOC**
  - *Progress Lakeshore*
- **OSHKOSH**
  - *Greater Oshkosh Economic Development Corporation*
- **SUPERIOR**
  - *Small Business Dev Center; UW Superior*

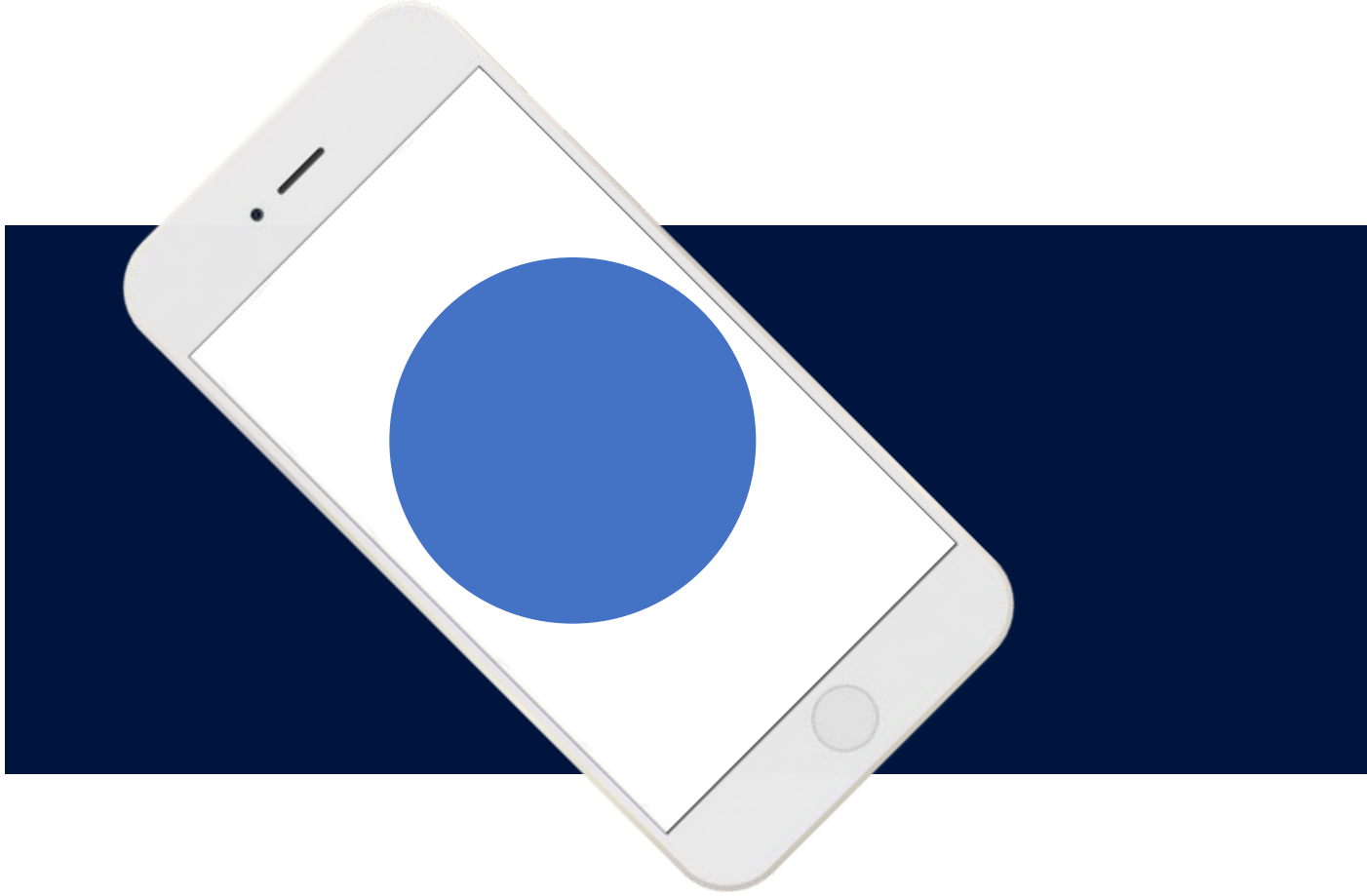



WPI Wisconsin Procurement Institute
An APEX Accelerator
Search ...
About
Events
Contracting with the Government
Cyber & Security
WPI Client Dashboard
Work with WPI
APEX ACCELERATORS
WISCONSIN APEX ACCELERATOR
UPCOMING EVENTS
APR 16 1:00 pm - 2:00 pm
Acquisition Hour: SAM.gov – Tools for Contracting
APR 24 9:00 am - 12:00 pm
Government Certification Workshop – State Certifications – Madison, WI
APR 24 12:00 pm - 1:00 pm
Acquisition Hour: Overview of the Contractor Performance Assessment Reporting System (CPARS)
APR 30 April 30, 2024 - May 3, 2024
Lieutenant Governor's Small Business Academy
MAY 16 8:00 am - 4:00 pm
10th Annual DoD Contract Management Update — Appleton, WI

The Federal Cybersecurity Horizon

Wisconsin Procurement Institute

AN APEX ACCELERATOR



August 28th, 2025

Agenda

01 **The Federal Position on Zero Trust**

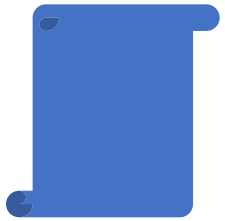
02 FedRAMP

03 Supply Chain Risk and SWFT

Why Now?

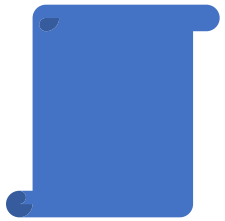
- **Evolving Adversaries; increased use of AI-enabled Tradecraft**
- EO 14028
- OMB M-22-09
- DOD Memo: DoD COTS Information and Communications Technology SCRM

Key Points: EO 14028



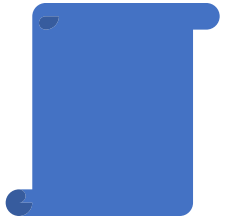
Modernize and Move to Zero Trust

Agencies must advance towards a Zero Trust Architecture and plan for cloud migration accordingly.



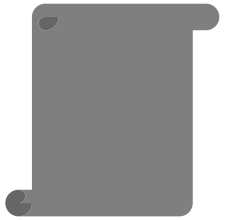
MFA & Encryption Mandate

All agencies must adopt multi-factor authentication and encrypt data regardless of system designation.



Cyber Safety Review Board

CSRB to review major incidents and recommend fixes.



EDR, SBOMS, etc

Mandates the implementation of more advanced EDR tools and the use of SBOMs, highlighting the importance of software as a key to government systems.

Key Points: OMB M-22-09

Modernize and Move to Zero Trust

Required agencies to meet specific cybersecurity objectives by end of FY 2024.

The Five Pillars

Goals were organized according to the Five Pillars of Zero Trust. Identity, Devices, Networks, Ampplications & Workloads, Data.

Zero Trust Lead

Must be designated within 30 days – submit a plan through FY 2024.

Only Going To Progress

Efforts to harden the DOD and Federal Agencies against Cyber Attacks have been a consistent push from the Executive level of the Federal Government since. 2012.

ExecutiveGov

KATIE ARRINGTON

Performing the Duties of
Chief Information Officer

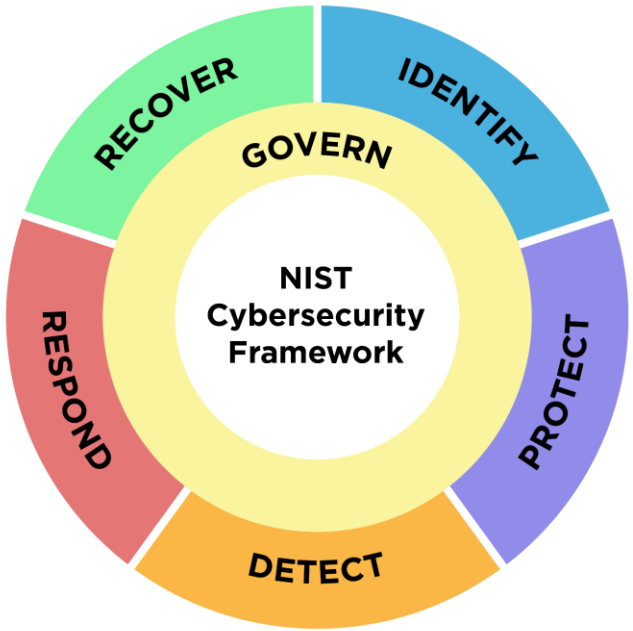
Department of Defense


LOCKHEED MARTIN
3103

The NIST Cybersecurity Framework (CSF) 2.0

National Institute of Standards and Technology
This publication is available free of charge from: https://doi.org/10.6028/NIST.CSWP.29
February 26, 2024

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE



1

NIST CSF 2.0

NIST Cybersecurity Framework (CSF) 2.0 – Mar 2025

2

CISA Implementation Report

CISA Zero Trust Architecture Implementation Report – Jan 2025

3

OMB M – 25 - 04

FY25 FISMA Guidance – pushing Zero Trust Maturity progress through 2025, aligning ZT Implementation with NIST CSF 2.0

Five Pillars:

Identity, Devices, Networks, Applications & Workloads, Data

The Alignment

NIST
National Institute of Standards and Technology

NIST SP 800-207
Zero Trust Architecture

NIST CSF 2.0

NIST CSF is being leveraged by the Federal Government as a governance methodology that includes the management and oversight of ZT Implementation.

ZT is now a tactical doctrine for how information systems are to be evaluated and secured.

Summary of Zero Trust Roadmap

- **Baseline:** Inventory, Identity Consolidation, Endpoint EDR, Logging
- **Build:** Risk-Based Access, Device Posture Gating, App-Level Authorization, Data Labeling
- **Scale:** Automation (SOAR), Continuous Verification, Policy-As-Code, Microsegmentation
- **Optimize:** Enterprise-wide Observability, Automated least-privilege, continuous ATO

Agenda

01 The Federal Position on Zero Trust

02 **FedRAMP**

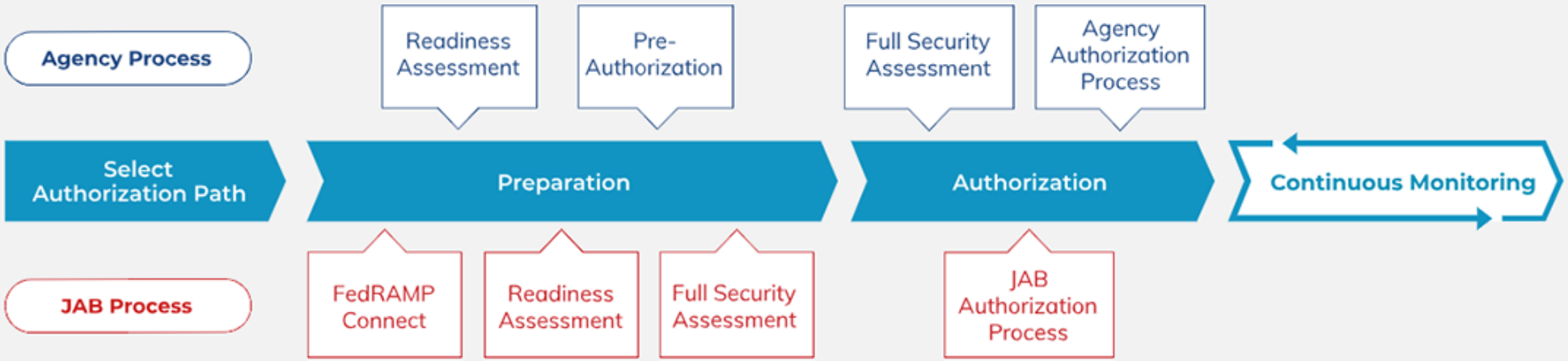
03 Supply Chain Risk and SWFT

Why Now?

- **Policy Refresh:** OMB M-24-15 clarified scope & roles.
- **FEDRAMP Authorization Act:** Formally codified the program into law.
- **Rev.5 Transition Process:** FEDRAMP baselines now aligned with NIST SP 800-52 Rev.5, including transition timelines.
- **Software Supply Chain:** Mandates for attestations and Common Form.

FedRAMP Authorization Process

There are two ways to authorize a Cloud Service Offering (CSO) through FedRAMP, through an individual agency or the Joint Authorization Board (JAB).



Note: Readiness Assessment is required for the JAB Process and is optional but highly recommended for the Agency Process.

Replace ARE with WERE – There is no JAB Process at this point in time.

So, uh, what changed?

Agency Authorizations are now almost exclusively the core path to validation.

The simplification of the Core Path to validation, combined with streamline of requirements, allow reuse of previous reviews.

The creation of new tools are meant to facilitate machine-readable artifacts and OSCAL usage to allow automation of review/assessment process.

Agenda

01 The Federal Position on Zero Trust

02 FedRAMP

03 **Supply Chain Risk and SWFT**

Why Now?

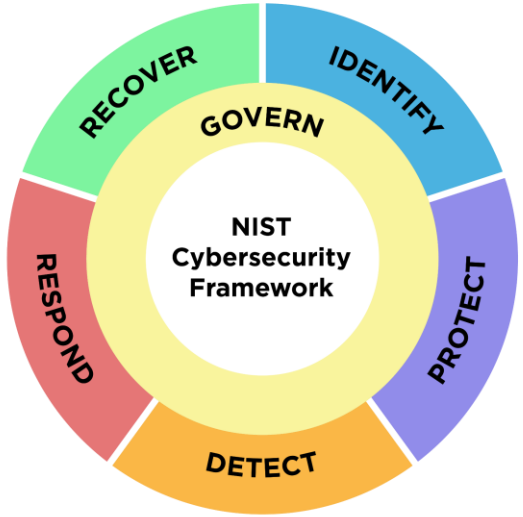
- **C-SCRM Tightening:** Rev.1 of NIST SP 800-161 refreshed the enterprise supply-chain practices.
- **Attestations are Live:** OMB/CISA's Secure Software Development Attestation is now in place.
- **DoD SWFT:** Software Fast Track (SWFT) following suit for DOD.
- **Paper to Data:** Software Assurance will require more due diligence, more rigorous ATOs, and better reuse.

OMB Requirements

- ❑Secure Software Attestations
- ❑Use NIST SSDF (SP 800-218) as baseline
- ❑Preference granted to vendors with VDPs, signed builds.

The Intentions Aligned

NIST
National Institute of Standards and Technology



What does the intention look like?

Problem: legacy VPN, flat networks, limited data visibility

Approach: app-level access, device posture gating, data discovery & labeling

FedRAMP SaaS for identity, logging; OSCAL-ready evidence; SSDF-aligned CI/CD

Outcome: reduced lateral movement & faster ATO/con-mon cycles, Supply Chain Secured and Validated (CMMC)

The Hang Ups

- ❑ Treating ZT as a tool purchase rather than a strategy
- ❑ Over-indexing on network controls; under-investing in identity & data
- ❑ Manual documentation and ad-hoc evidence → slows FedRAMP & CMMC audits
- ❑ Ignoring software producer attestations & provenance until acquisition

The CMMC Final Rule was published on **October 15, 2024**. It **BECAME** effective on **Dec 16, 2024**, and can now enter contracts and solicitations.

www.cyberab.org

48 CFR and Beyond

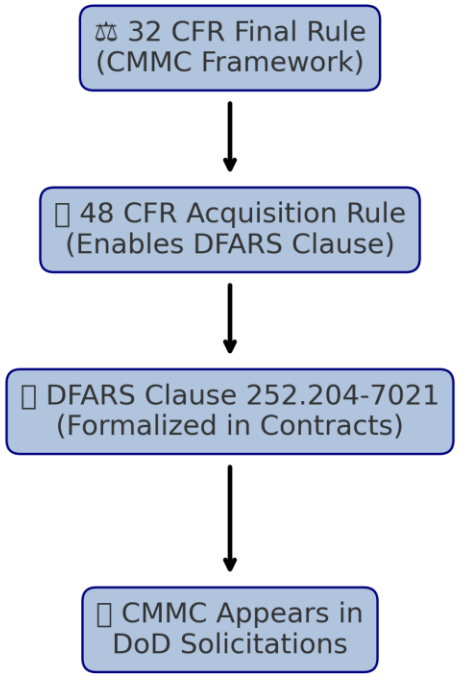
What is the 48 CFR?

- 48 Code of Federal Regulations
- Governs DoD acquisition regulations
- Enables DFARS clause 252.204-7021
- Addes CMMC Requirements to Solicitations

Current Status?

- Submitted to OIRA (Office of Information and Regulatory Affairs)
- Expected to Finalized by end of Q3
- Believed to have a 365 day implementation window

How the 48 CFR Rule Enables CMMC Enforcement

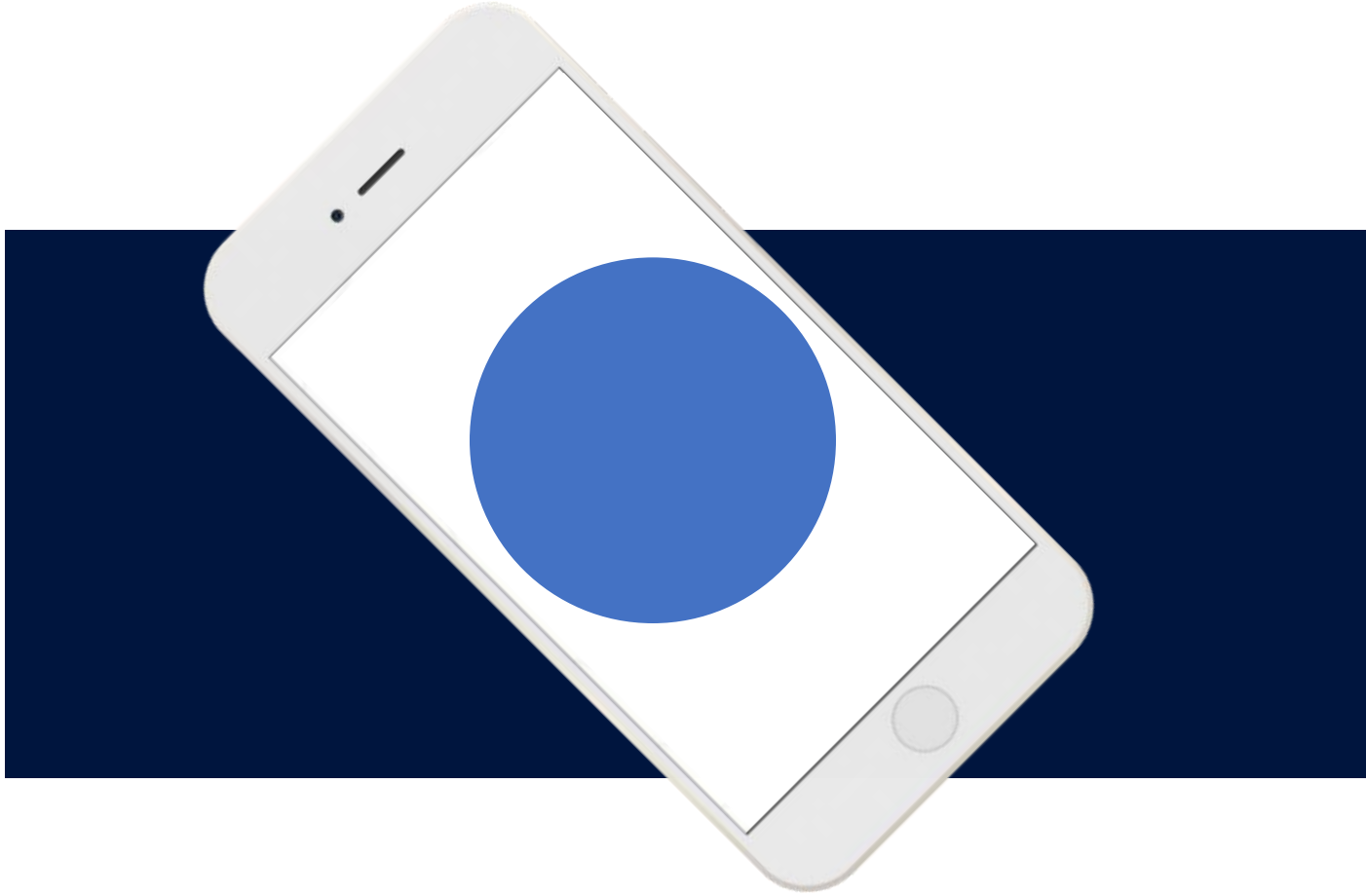


Matthew Frost

mattf@wispro.org

Wisconsin Procurement Institute

AN APEX ACCELERATOR



Upcoming Events

Acquisition Hour

The Acquisition Hour webinar series covers a range of topics from market entry, sales growth, small business certifications, compliance, and more. Attendees receive 1 CPE credit for attending.

- **September 10** – Contracting in Disasters Doing Business with Emergency Agencies
- **September 24** – Selling to the Government – is there an opportunity for your small business?
- **October 8** – The 8(a) Business Development Program
- **October 22** – Federal Acquisition Regulations (FAR) Overview
- **November 5** – Certification Programs for Women and Veteran Owned Businesses
- **November 12** – Getting Started w DLA/DIBBS for Contractor & Subcontractors Part 1
- **November 19** – Getting Started w DLA/DIBBS for Contractor & Subcontractors Part 2

…More information and registrations at wispro.org/events

Cyber Thursday

Cyber Friday is a series of one-hour webinars focusing on critical topics for DOD contractors and subcontractors in cyber security, data security, and CMMC. Attendees receive 1 CPE credit for attending.

- **August 28** – The Federal Cybersecurity Horizon: Zero Trust, FedRAMP, & Supply Chain Risk
- **September 25** – CMMC 2.0: What is 48 CFR and why it matters?
- **October 30** – CMMC and ITAR – Navigating the differences
- **November 20** – Federal Cyber Update – Review of current regulations

…More information and registrations at wispro.org/events

Featured Newsletters

Visit wispro.org to sign up for our monthly newsletters

Acquisition Alert | Cyber Newsletter Events Newsletter

August 28 2025

PRESENTED BY

Wisconsin Procurement Institute (WPI)

www.wispro.org

Matt Frost

Wisconsin Procurement Institute

MatthewF@wispro.org | 608-293-0920

10437 Innovation Drive Suite 320
Milwaukee WI 53226